2018年8月29日 星期三 周口晚报
组版编辑 关秋丽 E-mail/guanqiuli@126.com

百度公司董事长兼CEO李彦宏曾经在两会上畅想过智能车的未来:“只要把车开上高速,你就能吃着火锅唱着歌,被车轻轻松松地从北京载到上海。”360集团董事长兼CEO周鸿祎后来在公开场合“皮”了一下:“有一天,你吃着火锅唱着歌,可能智能车就被黑客劫持了。”周鸿祎素来喜欢“放炮”,但他描述的画面并非耸人听闻。

前不久,以色列一家汽车联网安全公司的CEO阿米·多坦说了这么一番话:“自动驾驶汽车系统可能会充满漏洞且易被黑客攻击。”

当车辆接入网络,也就给了黑客远程攻击的机会。360智能网联汽车安全实验室负责人刘健皓被称为“破解特斯拉第一人”,他曾发现特斯拉Autopilot(自动驾驶系统)存在传感器漏洞并将漏洞提交给了特斯拉公司的安全部门。刘健皓在接受记者采访时表示,漏洞不可避免,也不可能被完全清除,信息安全攻防是一场动态的持久战。

小心 你的联网车副驾驶上可能“坐”着黑客

存在漏洞和错误是代码的通病

阿米·多坦给出了这样一组数字:“联网汽车每1800行代码就会存在一些错误,其中80%是安全漏洞。”他还表示,一辆联网汽车和一辆自动驾驶汽车的潜在安全漏洞数目分别为5000和15000。

这是怎么算出来的?

北京理工大学网络攻防对抗技术研究所所长闫怀志告诉记者,国际著名的CMMI(软件能力成熟度集成模型)将软件能力成熟度分为5级,其中1级最低,5级最高,4级和5级的千行代码缺陷率分别为0.92‰和0.32‰。联网汽车“每1800行代码就存在一些错误”,表明其软件能力成熟度大致在CMMI 4级和5级之间。“虽然联网汽车代码成熟度达到了较高水平,但显然还有一定的提升空间。”闫怀志说。

闫怀志认为,软件代码出现漏洞,是由软件开发和应用过程中的不正确或遗漏行为所造成的,也就是在软件设计、实现或应用过程中有意或无意导致软件架构或其具体实现与期望不符。“漏洞的出现是所有软件代码的通病,不仅仅局限于联网汽车与自动驾驶应用领域。”不过,漏洞出现的频率又跟软件研发和保障水平密切相关。比如,在级别不同的CMMI研发保障能力下开发出来的代码质量和漏洞数量会有显著差异。“自动驾驶软件属于典型的工业应用软件之一,其安全漏洞的潜在危害性尤其是对人和物理环境的破坏性都极大,和普通软件的危害不能同日而语。”闫怀志强调。

有漏洞不是稀奇事。中国科学院微电子研究所副研究员王云表示,随着汽车智能化水平的提高,一辆车上的代码可能有几千万甚至上亿行,存在错误和漏洞是肯定的。“不光自动驾驶行业,传统软件行业都会有各种错误,不管是Windows还是iOS。”

车载娱乐系统易成被侵入对象

漏洞是如何被发现和修复的?

王云介绍,成熟的软件开发都会有标准流程,会对需求、架构设计方案、代码模块设计接口、代码机制等环节进行代码测试与评审。通过规范的流程,大部分代码漏洞可以被发现,但是依然有少部分漏洞不会被测试用例覆盖。

“联网汽车涉及各种协议或操作系统、应用软件,存在漏洞的地方更多。目前被发现的漏洞涉及TSP(内容服务提供商)平台、APP应用、Telematics Box(T-BOX)上网系统、车机IVI系统CAN-BUS车内总线等各个领域和环节。”王云表示,协议、操作系统存在的漏洞都可能被利用,造成的危害也不一样:有的能让黑客窃取用户信息,更严重的能让黑客控制汽车。

刘健皓把漏洞比喻为银行的后门,大门处有重兵把手,但后门可能就是防护真空。“有心人士”能通过后门大摇大摆进来“搞事情”,而且,很可能银行自己都不知道有这个后门。

车联网及自动驾驶软件实现了车-车之间、车-人之间、车-路之间的高效互联互通与信息共享,并为车联网智能决策和优化提供了基础支撑,但它也让联网车在信息安全、功能安全及隐私保护等方面面临着前所未有的严峻挑战。闫怀志说,黑客可以利用车载终端系统、车联网云平台、移动APP、OBD(车载诊断系统)等系统的漏洞对车辆实施攻击,实现对智能车辆的操作控制。不安全的代码也可能在无攻击的情况下“自行”失效,导致车辆行为失控。

“有通信、接口的地方就容易遭到攻击。”刘健皓说,黑客攻击车辆可以分为物理接触、近场控制、远程控制3种。在智能网联时代,黑客能“顺着网线”悄无声息地进入你的车。

在测试联网汽车时,刘健皓团队也发现,车载娱乐系统易成为被侵入的对象。如今,汽车的中控系统做得越发酷炫,为了给用户更为高科技的人机交互体验,一些实体控制按钮被集成到了车载娱乐系统当中,该系统通常也要为用户提供互联网内容。于是,黑客就能通过车载娱乐系统的漏洞,一举控制车辆的仪表盘甚至制动系统。

从已有的案例来看,最夸张的情况是:黑客能控制车辆动力和转向系统。比如远程启动一下发动机,比如让你的方向盘有“自己的想法”。而且,如果黑客破解了某车厂的后台,他就能用同样的方法横向批量影响到所有该品牌的汽车。所以,如果有汽车在道路上集体“抽风”,也不是不可能。

打一场动态信息安全攻防战

当然,如果真“集体抽风”,就成了公共安全事件,一切都要防患于未然。联网车并不只是黑客的猎物,实际上,车厂也会采取种种措施升级自己的防护机制。与入侵者斗智斗勇,本身就是一个你来我往、你攻我挡的动态平衡过程。

“安全防护不只是防护某个‘点’,一定要做到全面。”刘健皓说。所谓的全面,指的是在云(云服务)、管(通信)、端(车载终端)、控(控制系统)上全面保驾护航。

闫怀志表示,代码错误的避免和纠正,需要标本兼治,且应以治本为主、治标为辅。“标”是采用各种漏洞挖掘、分析、测试及修复手段来避免或减缓其安全威胁;“本”上还是应该严格遵循软件安全工程规范,从源头上解决问题。尤其是对于车联网和自动驾驶这种工业软件来说,要特别重视功能安全与信息安全二者的结合,从其全生命周期统一考虑各种安全因素。“具体来说,是识别工业应用软件的危险,定义其安全需求,然后进行安全设计、安全编码及安全测试,进行有效的缺陷管理,即实施基于功能安全与信息安全融合的工业应用软件安全工程方法。”

闫怀志介绍,在进行具体安全设计和代码编写时,可参考多种安全编码标准和指南。比如,汽车行业可以参考汽车电子功能安全标准(ISO 26262),还可以参考国际著名的MISRA(汽车工业软件可靠性联合会)的工业C编程规范。“该规范为汽车嵌入式系统编码提供了有关安全可靠性的最佳实践。”闫怀志说。

王云透露,国际组织(ISO/SAE)正进行21434(道路车辆—信息安全工程)标准的制定。该标准主要从风险评估管理、产品开发、运行/维护、流程审核等4个方面来保障汽车信息安全工程工作的开展。

在具体实践上,360智能网联车安全实验室给车企的建议是——“逆向思维”。在车辆正式推出之前,他们会对合作车企车辆进行测试,模拟黑客对车辆进行攻击;发现漏洞后,让车企对薄弱环节进行修正。车辆上市后,团队会为车辆做全生命周期的安全管理,监控和防护其可能遭到的攻击。

“没有一个安全公司能够保证车辆百分之百安全,跟黑客对抗的过程是动态防护的过程:发现攻击、阻断攻击、下发更新策略……”刘健皓强调,“我们希望为每个车厂建立一套安全的运营体系,实现自主品牌车辆的安全运营”。

(据《科技日报》)